Deutscher Bundestag **Drucksache 17/6802**

17. Wahlperiode 16. 08. 2011

Kleine Anfrage

der Abgeordneten Agnes Malczak, Omid Nouripour, Tom Koenigs, Dr. Konstantin von Notz, Marieluise Beck (Bremen), Volker Beck (Köln), Viola von Cramon-Taubadel, Thilo Hoppe, Uwe Kekeritz, Katja Keul, Ute Koczy, Kerstin Müller (Köln), Lisa Paus, Claudia Roth (Augsburg), Manuel Sarrazin, Dr. Frithjof Schmidt, Hans-Christian Ströbele und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Cyber-Strategie und Cyber-Außenpolitik der Bundesregierung

Die „Cyber-Sicherheitsstrategie für Deutschland“ der Bundesregierung vom Februar 2011 betrachtet den Schutz des Cyber-Raums als existentielle Frage des 21. Jahrhunderts. Um Sicherheit im Cyber-Raum zu gewährleisten, strebt sie eine enge internationale Zusammenarbeit an, und hebt hierbei insbesondere die NATO (North Atlantic Treaty Organization) hervor. Nach Behördenangaben und Meinung von Expertinnen und Experten hat die Bedrohung des Cyber-Raums in jüngster Zeit zugenommen und mit neuen, insbesondere staatlichen Akteuren eine neue Qualität erreicht. Als eine Antwort eröffnete das Bundesministerium des Innern am 16. Juni 2011 das nationale Cyber-Abwehrzentrum, mit dem künftig schneller auf Angriffe reagiert und das Krisenmanagement optimiert werden soll.

Es gibt berechtigte Zweifel, ob die Strategie der Bundesregierung und das neue Cyber-Abwehrzentrum geeignet sind, die Sicherheit des Cyber-Raums in Deutschland zu verbessern. Es fehlt an technischer Expertise und Ressourcen, um komplexe und gefährliche Angriffe überhaupt zu erkennen und darauf zu reagieren. Auch bezüglich der konkreten Ausgestaltung der internationalen Zusammenarbeit im Cyber-Raum herrscht weitestgehend Unklarheit. Die Beschreibung der Cyber-Außenpolitik der Bundesregierung bleibt vage hinsichtlich Form und Inhalt der von der Bundesregierung angestrebten Abstimmungen, Regulierungen, Kontrollen und Verhaltensnormen sowie der Zuständigkeiten auf internationaler Ebene.

Vor dem Hintergrund der von der Bundesregierung skizzierten Bedrohungslage und angesichts der Aufrüstungsdynamik im Cyber-Raum, fragen wir daher die Bundesregierung.

Wir fragen die Bundesregierung:

Grundsätzliche Fragen zur Cyber-Strategie

1. Welche Maßnahmen, Fähigkeiten und Mittel stellt die Bundesregierung bisher konkret zur Prävention und zum Schutz vor Cyber-Angriffen sowie zur Wiederherstellung und zur Reaktion auf derartige Angriffe bereit?

2. Welche Maßnahmen hat die Bundesregierung ergriffen, um die Bund-Länder-Kooperation im Bereich Cyber-Sicherheit zu verbessern und ein effektives Krisenmanagement im Fall eines Angriffs zu gewährleisten?

3. Welche Maßnahmen ergreift die Bundesregierung zur Erhöhung des Selbstschutzes gegen Cyber-Angriffe?

   a) Welche Maßnahmen plant sie zur Verbesserung des Meldesystems für den Informationsaustausch?

   b) Welche Maßnahmen unternimmt sie zur Reduktion der Anzahl von Schnittstellen zwischen Netzen?

   c) Welche Maßnahmen plant sie hinsichtlich der Dezentralisierung und Diversifikation der IT-Systeme (IT = Information Technology)?

   d) Welche Maßnahmen unternimmt sie zum Aufbau von doppelten und mehrfachen Sicherungssystemen (IT-gestützt oder IT-unabhängig) im Bereich kritische Infrastruktur?

4. Inwiefern ist nach Ansicht der Bundesregierung eine Trennung von offensiven und defensiven Fähigkeiten im Bereich Cyber-Sicherheit möglich?

   Wie definiert sie in diesem Kontext offensive und defensive Fähigkeiten?

5. Hält die Bundesregierung einen digitalen Angriff für einen bewaffneten Angriff im Sinne des Völkerrechts, und wenn ja, wie begründet sie dies?

6. Erfordert der Einsatz von Cyber-Fähigkeiten seitens der Bundeswehr nach Ansicht der Bundesregierung eine Mandatierung durch den Deutschen Bundestag, und wie begründet die Bundesregierung ihre Auffassung?

7. Kann ein Cyber-Angriff vor dem Hintergrund des Rückverfolgungsproblems nach Ansicht der Bundesregierung einen möglichen Fall individueller oder kollektiver Selbstverteidigung im Sinne des Völkerrechts auslösen, und wenn ja, wie begründet sie dies?

Grundsätzliche Fragen zur Cyber-Außenpolitik

8. Welche Form, und welchen Inhalt sollten internationale Regulierungen zur Verbesserung der Sicherheit im Cyber-Raum nach Ansicht der Bundesregierung haben?

9. Welche Foren und Organisationen auf internationaler Ebene sollten hierbei nach Auffassung der Bundesregierung für jeweils welche Bereiche zuständig sein (bitte insbesondere auf die Vereinten Nationen (VN), die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), die Europäischen Union (EU), der Europarat, die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) oder die NATO eingehen)?

10. Welche Position vertritt die Bundesregierung hinsichtlich der verschiedenen möglichen Formen internationaler Kooperationsvereinbarungen?

    a) Welche Position vertritt sie hinsichtlich der Schaffung eines Rüstungskontrollregimes für den Cyber-Raum?

    b) Welche Position vertritt sie hinsichtlich der Schaffung verbindlicher Verhaltensnormen und Regeln zum Umgang mit Cyber-Angriffen und gemeinsamen Krisenmanagement?

    c) Welche Position vertritt sie hinsichtlich der Schaffung vertrauensbildender Maßnahmen, insbesondere zur Schaffung von Transparenz?

    d) Welche Position vertritt sie hinsichtlich der Schaffung gemeinsamer Fähigkeiten für Cyber-Angriffe mit Partnerländern bzw. im Rahmen von internationalen Organisationen und Bündnissen?

11. Welche Initiativen hat die Bundesregierung auf welchen Ebenen, und mit welchen Ergebnissen bisher unternommen, um die internationale Zusammenarbeit zur Verbesserung der Sicherheit im Cyber-Raum voranzutreiben (bitte einzeln auf VN, OSZE, EU, Europarat, OECD und NATO eingehen)?

12. Welche Anstrengungen mit welchen Ergebnissen hat die Bundesregierung bisher unternommen, um einen möglichst universellen Kodex für staatliches Verhalten im Cyber-Raum (Cyber-Kodex) zu etablieren, der auch vertrauens- und sicherheitsbildende Maßnahmen umfasst?

    Welchen Inhalt haben die von der Bundesregierung im Rahmen der Cyber-Sicherheitskonferenz der OSZE im Mai 2011 gemachten Vorschläge der Bundesregierung für einen Verhaltenskodex?

13. Worin liegen nach Auffassung der Bundesregierung die Schwierigkeiten bei der Etablierung eines solchen Kodexes, und durch welche Vorgehensweise versucht sie diese zu beseitigen?

14. Wie bewertet die Bundesregierung die Empfehlung von Expertinnen und Experten zu einer internationalen Vereinbarung, nach der ein angegriffener Staat unverzüglich und umfassend über den Angriff informieren und infizierte Rechner vom Netz nehmen sollte?

    Auf welcher Ebene sollten solche Vereinbarungen nach Einschätzung der Bundesregierung getroffen werden?

15. Auf welcher Ebene strebt die Bundesregierung internationale Standards für das Krisenmanagement im Fall von Cyber-Angriffen an?

    a) Für welche Aspekte des Krisenmanagements befürwortet die Bundesregierung globale Standards?

    b) Welche konkreten Vorschläge hat die Bundesregierung hierzu, und in welchem Rahmen setzt sie sich dafür ein?

    c) Was hat sie auf Ebene der VN diesbezüglich unternommen?

16. Was hat die Bundesregierung bisher unternommen, und welche Maßnahmen plant sie, um die Transparenz im Bereich militärischer und nachrichtendienstlicher Fähigkeiten im Cyber-Raum zu verbessern (bitte insbesondere auf die USA, China, Russland und Großbritannien eingehen)?

17. Wie bewertet die Bundesregierung die Idee, Frühwarnsysteme in Form automatischer Sensorennetzwerke und Hotlines zwischen Staaten auszubauen?

    Was hat sie in dieser Richtung bisher unternommen, und welche Maßnahmen plant sie?

18. Wie bewertet die Bundesregierung die russische Initiative für einen Rüstungskontrollvertrag für den Cyber-Raum?

    a) Welche Konsultationen mit Russland und anderen Staaten fanden hierzu bisher statt, und mit welchen Ergebnissen?

    b) Welche Schritte plant die Bundesregierung in diese Richtung?

19. Welche Position vertritt die Bundesregierung hinsichtlich der Forderung der VN-Generalversammlung zur Schaffung einer globalen Kultur der Cyber-Sicherheit und zum Schutz kritischer Informationsinfrastrukturen (Resolution 58/199, 30)?

    Was unternimmt die Bundesregierung hierzu auf Ebene der VN?

20. Welche Position vertritt die Bundesregierung hinsichtlich des US-amerikanischen Vorschlags für rechtlich unverbindliche Verhaltensnormen und vertrauensbildende Maßnahmen?
21. Was unternimmt die Bundesregierung, um neben euro-atlantischen Institutionen (EU, NATO) auch asiatische und afrikanische Organisationen in die internationalen Abstimmungsprozesse im Bereich Cyber-Sicherheit einzubeziehen (Vereinigung südostasiatischer Staaten zur Förderung von Frieden und Wohlstand – ASEAN, Afrikanische Union)?
22. Welche Organisationen stehen für die Bundesregierung bei der internationalen Kooperation im Bereich Cyber-Sicherheit im Mittelpunkt?

Fragen zur Cyber-Außenpolitik im Rahmen der NATO

23. Welche Aufgaben soll die NATO aus Sicht der Bundesregierung hinsichtlich des Themas Cyber-Security übernehmen, wie soll die NATO dies nach Ansicht der Bundesregierung tun, und wie versucht die Bundesregierung, dies im Verbund mit den Partnerländern auf NATO-Ebene umzusetzen?
24. Welche Position vertritt die Bundesregierung auf NATO-Ebene bezüglich einer Ächtung des Einsatzes von elektronischer Datenverarbeitung und Telekommunikation zur direkten oder flankierenden Kriegsführung?
25. Welche Eckpunkte enthält die NATO Cyber Defense Policy vom 8. Juni 2011?
    a) Welche Cyber-Sicherheitsmaßnahmen sieht die NATO Cyber Defense Policy vor?
    b) Welche Grundsätze und Standards sieht die NATO Cyber Defense Policy vor?
    c) Inwiefern enthält die NATO Cyber Defense Policy auch Empfehlungen bzw. Standards für den Austausch von Information über Schwachstellen?
26. Welche unterschiedlichen Ansichten unter den Mitgliedstaaten gibt es bezüglich Strategie und aufzubauenden Fähigkeiten der NATO im Bereich Cyber-Sicherheit?
27. Welchen konkreten inhaltlichen Beitrag hat die Bundesregierung zur NATO Cyber Defense Policy geleistet?
28. Welche Stelle der Bundesregierung hat diesen Beitrag geleistet, und welche Institutionen und Bundesministerien waren involviert?
29. Welche Gremien und Agenturen sind für die geplante Ausarbeitung des detaillierten Arbeitsplans zur Umsetzung der NATO Cyber Defense Policy vorgesehen?
    a) Wer nimmt hieran für die Bundesrepublik Deutschland teil, und welche Institutionen und Bundesministerien sind involviert?
    b) Welche inhaltliche Zielsetzung verfolgt die Bundesregierung hierbei?
30. Welche Maßnahmen ergreift die Bundesregierung, um bei der Umsetzung der NATO Cyber Defense Policy die Trennung von militärischen und polizeilichen Aufgaben zu wahren?
31. Welche Positionen vertritt die Bundesregierung hinsichtlich der Befassung der NATO mit der Bekämpfung von Internetkriminalität, wie es das neue strategische Konzept der NATO vorsieht?

32. Welchen Beitrag leistet die Bundesregierung im Rahmen ihrer Beteiligung am NATO Cooperative Cyber Centre of Excellence in Tallinn, und mit welchem Personal ist sie dort vertreten?

33. Inwiefern hält die Bundesregierung den Aufbau der Cyber Defence Management Authority (CDMA) der NATO für sinnvoll und notwendig?

    a) Welche Aufgaben und Funktionen hat die CDMA derzeit, und wie ist sie personell besetzt (sowohl ziviles als auch militärisches Personal)?

    b) Wie hat die Bundesregierung den Aufbau bisher unterstützt?

    c) Wie beteiligt sich die Bundesregierung derzeit personell und finanziell?

    d) Inwiefern treffen Berichte zu, wonach die CDMA ausgebaut werden soll in „a war-room operation for NATO's cyber defences with actual tactical responses carried out by member states through a ‚coalition of the willing'"[1]?

    e) Inwiefern unterstützt die Bundesregierung eine solche Entwicklung bzw. heißt sie gut?

34. Wie bewertet die Bundesregierung das am 10. März 2011 bei einem Treffen der NATO-Verteidigungsminister in Brüssel gebilligte Cyber Defence Concept der NATO?

    Welche Schlussfolgerungen zieht die Bundesregierung für den Aufbau und Vorhalt nationaler, sowohl ziviler als auch militärischer Kapazitäten, die im NATO-Verbund bereitgestellt werden sollen?

Fragen zur Cyber-Außenpolitik im Rahmen der EU

35. Was hat die Bundesregierung unternommen, um die vom Wirtschafts- und Sozialrat der Europäischen Union kritisierte Uneinheitlichkeit und mangelnde Koordination innerhalb der EU beim Schutz kritischer Infrastrukturen zu beheben?

36. Welche Initiativen hat sie ergriffen, um die ebenfalls vom Wirtschafts- und Sozialrat angemahnte Transparenz von Sicherheitslücken und -problemen zu verbessern?

37. Was unternimmt die Bundesregierung, um die Europäische Agentur der Informations- und Netzsicherheit, wie von der Europäischen Kommission gefordert, zu stärken?

38. Welche Position vertritt die Bundesregierung hinsichtlich der Forderung des Europäischen Parlaments nach einer „Europäische Strategie für Computer- und Netzsicherheit", und welche Initiativen hat sie in dieser Richtung unternommen?

Berlin, den 16. August 2011

Renate Künast, Jürgen Trittin und Fraktion

---

[1] Vgl. Hughes, Rex B.: NATO and Cyber Defence, Atlantisch Perspectief, 2009, Nr.1/8.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333